UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,068	10/11/2001	Tim M. Hoberock	10010811-1	1566

7590 03/31/2008

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
03/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/976,068
Filing Date: October 11, 2001
Appellant(s): HOBEROCK ET AL.

Steven L. Nichols
Reg. No. 40,326
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 26 December 2007 appealing from the Office action mailed 26 September 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Lopes U.S. Patent No. 6,189,105 – issued 13 Feb. 2001 – "In accordance with the principles of the present invention, a proximity detection system for a computer comprises means for enabling a computer when a valid user is present, and means for disabling the computer when the valid user is not present. In another aspect, a proximity detection system comprises a proximity detector in communication with the computer. A timer associated with the computer is operable to expire upon non-receipt of an authorizing code from an authorized user of the computer. A disabling

module in the computer disables at least one feature of the computer based on an expiration of the timer". (col. 2, lines 15-26)

Gulick et al. U.S. Patent 6,823,451 – issued 23 Nov. 2004 – "A device for security and manageability. The device includes a port, one or more secured assets; and security hardware. The port is configured to receive at least one operating mode signal. The at least one operating mode signal is indicative of a first operating mode. The security hardware is coupled to receive the at least one operating mode signal. The security hardware is further coupled to control access to the secured assets dependant upon the at least one operating mode signal. Another device includes first bus interface logic for coupling to a first external bus, a port, one or more secured assets, and security hardware coupled to control the one or more secured assets" (Abstract)

Kolls U.S. Patent 6,609,102 – issued 19 Aug. 2003 – teaches that a "PC 630 can be a specialized PC, which through software prevents a user from functionally using the PC 630 until a satisfying condition or state, is presented. Upon receipt of the satisfying criteria, PC 630 by way of software intervention allows a user to functionally use the PC 630. A unique feature of this form of PC is that while software grants and denies access to the PC system, software continues to oversee the user's activities, choosing to intervene and prevent the user from performing certain functions. Functions that can be blocked are those that comprise system security, including access to hardware, access to hardware settings, access to software, and or access to software settings. This specialized form of a PC 630 can generally be referred to as a public PC" (from col. 6, lines 19-34).

Note: All of the above references teach restricting access to a computer

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-3, 6, 9-11, 14, and 16, are rejected under 35 U.S.C. 102(a) as being anticipated by Lopes U.S. Patent No. 6,189,105 (hereinafter '105).

Regarding independent claim 9,

As per the first limitation, **"A method for controlling use of a piece of office equipment or a particular resource available through that piece of equipment, said method comprising: timing a period during which said equipment receives no user input and placing said equipment or a resource available through said equipment into a locked state upon elapse of a pre-determined period during which no user input is received"** is taught in '105 col. 2, lines 14-26.

As per the second limitation, **"re-enabling operation of said piece of office equipment or a resource available through that office equipment to an authorized user upon presentation of an identifier of said authorized user to a sensor of a lock control device connected to said piece of office equipment, wherein said sensor senses and recognizes said identifier to identify said authorized user"** is shown in '105 col. 2, lines 27-35.

Regarding claim 10, **"wherein said piece of office equipment is a computer or computer terminal"** is disclosed in '105 col. 2, line 16.

Regarding claim 11 **"further comprising using a proximity card sensor as said lock control device"** is taught in '105 col. 3, lines 14-31.

Regarding claim 14 **"further comprising accessing a particular application residing on said computer or accessible through said computer terminal by presenting an identifier of said authorized user to said sensor of said lock control device"** is shown in '105 col. 3, lines 52-62.

Regarding claim 16 **"further comprising: timing periods during which said computer or computer terminal receives no user input; locking up or logging out said computer upon elapse of a pre-determined period during which no user input is received; and unlocking or logging in said computer upon operation of said lock control device"** is disclosed in '105 col. 4, lines 33-51.

Regarding independent claim 1, this claim is directed to a system of the method of 9; therefore it is rejected along similar rationale.

Regarding claims 2, 3, and 6, these claims contain substantially similar subject matter as claims 10, 11, and 14; therefore they are rejected along the same rationale.

Claims 21 and 25, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lopes U.S. Patent No. 6,189,105 (hereinafter '105).

Regarding dependent claims 21 and 25, **"further comprising: initially unlocking said computer or computer terminal with entry of at least one password; and allowing a user to subsequently unlock said computer or computer terminal by presentation of said user identifier rather than re-entry of said at least one password"** is taught in '105 teaches col. 8,
lines 10-22 "the present invention does not preclude and in fact prefers the use of passwords in addition to the continuous authorization in accordance with the principles of the present invention to provide increased security" in addition "those skilled in the art will be able to make various modification to described embodiment of the invention without departing from the true spirit and scope of the invention".

Claims 22 and 26, are rejected under 35 U.S.C. 103(a) as being unpatentable over 'Lopes U.S. Patent No. 6,189,105 (hereinafter '105).

Regarding independent claim 26,

As per the first limitation, **"A method for controlling use of a piece of office equipment or a particular resource available through that piece of equipment, said method comprising: timing a period during which said equipment receives no user input and placing said equipment or a resource available through said equipment into a locked state upon elapse of a pre-determined period during which no user input is received; and "** is taught in '105 col. 2, lines 14-26.

As per the second limitation, **"re-enabling operation of said piece of office equipment or a resource available through that office equipment to an authorized user upon presentation of an identifier of said authorized user to a sensor of a lock control device connected to said piece of office equipment, wherein said sensor senses and recognizes said identifier to identify said authorized user"** is shown in '105 col. 2, lines 27-35.

As per the third limitation, **"said method further comprising: initially unlocking said computer or computer terminal with entry of at least one password; allowing a user to subsequently unlock said computer or computer terminal by presentation of said user identifier rather than re-entry of said at least one password; and"** is disclosed in '105 col. 8,
lines 10-22 "the present invention does not preclude and in fact prefers the use of passwords in addition to the continuous authorization in accordance with the principles of the present invention to provide increased security" in addition "those skilled in the art will be able to make various modification to described embodiment of the invention without departing from the true spirit and scope of the invention"

As per the fourth limitation, **"unlocking said piece of office equipment with said identifier for a second predetermined period after entry on of said at least one password, with re-entry of said password being required to unlock said piece of office equipment after elapse of said second predetermined period of time, said second predetermined period of time being longer than said first predetermined period of time"** is taught in '105 col. 5, lines 23-39 "Step 212 checks the value of the security counter to determine if it is time to check for the

presence of the proximity badge 100. If the security timer has not yet reached its present maximum value (determined by the user based on their particular needs), then step 2112 repeats. Once the security counter has reached the maximum count, i.e., the point at which it is desired to check for the presence of the proximity badge 100, then the process return to step 202 to search for the receipt of the coded message" in as well as '105 teaches in col. 8, lines 10-22 that alteration with password and variations are within the scope of the invention.

Regarding independent claim 22, this claim is directed to a system of the method of claim 26; therefore it is rejected along similar rationale.

Claims 4, 5, 7, 12, 13, 15, 24, and 28, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lopes U.S. Patent No. 6,189,105 (hereinafter '105) in view of Gulick et al. U.S. Patent No. 6,823,451 (hereinafter '451).

Regarding claim 12, **"further comprising using a magnetic card reader as said lock control device"** is taught in '451 col. 8, lines 46-56 that a card reader as a lock control device.

Regarding claim 13, **"further comprising connecting said lock control device to said computer or computer terminal via a connector that also connects a keyboard to said computer or computer terminal"** is disclosed in '451 col. 8, lines 46-56 and '451 col. 1,
lines 57-65.

Regarding claim 15, **"further comprising accessing a network server on a computer network to which said computer is connected by presenting an identifier of said authorized user to said lock control device"** is shown in '451 col. 47, line 59 through col. 48, line 3.

Regarding claim 28, **wherein said identifier comprises a biological characteristic of said user"** is shown in '451 col. 8, lines 46-56.

Regarding claims 4, 5, 7, and 24, these claims contain substantially similar subject matter as claims 12, 13, 15, and 28; therefore they are rejected along similar rationale.

Claims 23 and 27, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lopes U.S. Patent No. 6,189,105 (hereinafter '105)in view of Kolls U.S. Patent No. 6,609,102 (hereinafter '102).

Regarding independent claim 27,

As per the first limitation, **"A method for controlling use of a piece of office equipment or a particular resource available through that piece of equipment, said method comprising: timing a period during which said equipment receives no uses input and placing said equipment or resource available through said equipment into a locked state upon elapse of a pre-determined period during with no use input is received; and"** is taught in '105 in col. 2, lines 14-26.

As per the second limitation, **"re-enabling operation of said piece of office equipment or a resource available through that office equipment to an authorized user upon presentation of an identifier of said authorized user to said sensor of a lock control device connected to said piece of office equipment, wherein said sensor senses and recognizes said identifier to identify said authorized user"** is shown in '105 col. 2, lines 27-35.

As per the third limitation, **"where said identifier comprises a credit card"** is taught in '102 col. 5, lines 16-43 the use of a credit to operate office equipment such as a PC in.

Regarding independent claim 23, this claim is directed to a system of the method of claim 27; therefore it is rejected along similar rationale.

(10) Response to Argument

Regarding Applicant's first argument, beginning on page 14, *"Thus, Lopes teaches disabling the use of a computer upon failure to detect a coded message on a badge, i.e., proximity card, worn by an authorized user. Lopes has not been shown to teach or suggest the claimed system or method including "placing said equipment or resource available through said equipment into a locked state upon elapse of a pre-determined period during which no user*

input through a keyboard or mouse is received." Clearly, locking a computer upon failure to detect a proximity card is different that locking a computer due to lack of input through a keyboard or mouse as claimed".

The Examiner disagrees with argument, the portion of the claim underlined above is well known in the art as a screen saver with locking feature, this is taught in Lopes in addition see below.

From Lopes col. 2, lines 20-26

"In another aspect, a proximity detection system comprises a proximity detector in communication with the computer. A timer associated with the computer is operable to expire upon non-receipt of an authorizing code from an authorized user of the computer. A disabling module in the computer disables at least one feature of the computer based on an expiration of the timer"

From Lopes col. 6, lines 39-47

"In addition, the proximity system may include a detection of the presence of an object (i.e., a person) synchronously with the detection of an authorized proximity detector. For instance, FIG. 4 shows a process for synchronously detecting the presence of a person in proximity to the computer together with a check of authority of the detected person. In FIG. 4, presence of a person is detected in step 482. Presence may be determined in any of a number of ways, e.g., by detection of a keypress on the keyboard."

Regarding Applicant's second argument beginning on page 14, *"The recent Office Action refers to Lopes at col. 6, lines 38-50 (Action, p. 3). This portion of Lopes merely teaches that when detecting the presence of proximity card, the system can also additionally detect the corresponding presence of a person using, for example, input from a keyboard. According to Lopes, "the proximity system may include a detection of the presence of an object (i.e., a person synchronously with the detection of an authorized proximity detector ... and certainly does not change the fact that Lopes primarily teaches the continuous detection of a proximity card as a requirement for granting system access".*

The Examiner disagrees with argument. Lopes teaches using a proximity card to access a system. Lopes also teaches utilizing a timer to monitor the period of time before placing the computer in a locked state. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123). A screen saver is well known in the art and Lopes teaches that other modes of protection can be utilized such as passwords and screen savers see col. 4, lines 52-54 "For instance, the computer function disabled in step 206 may operate as a screen saver to prevent visual display of information on the display 112 when the proximity badge 100 is not in the proximity of the proximity reader 120"and col. 8, lines 13-16 "While all embodiments herein provide continuous security of a computer (as opposed to the conventional method of password entry to provide a one-time authority check), the present invention does not preclude and in fact prefers the use of passwords in addition to the continuous authorization in accordance with the principles of the present invention to provide increased security". The Lopes invention is in addition to the methods already available such as screen savers. It is not a patentable difference that Lopes does not teach the screen saver functionality, because this is already well know in the art.

Regarding Applicant's third argument beginning on page 15, *"Lopes does not teach or suggest, nor is it inherent in Lopes that the computer is placed into a locked state based on a lack of user input through a keyboard or mouse as claimed".*

The Examiner disagrees with argument, Lopes teaches that the presence of a user is detected and if the user is not present the computer is placed into a locked state. One of the ways the presence of a user is detected is by entry in a

keyboard entry see col. 6, lines 45-47. "In FIG. 4, presence of a person is detected instep 482. Presence may be determined any of number of ways, e.g., by detection of a keypress on the keyboard".

Regarding Applicant's fourth argument beginning on page 15, directed to claims 21, 22, 25, 26, 4, 5, 7, 12, 13, 15, 24, and 28 *"Thus, Appellant recites, not just initially unlocking a piece of office equipment with a password, but timing a "second predetermined period of time" during which the password need not be re-entered if another identifier, as claimed is used. The recent Action consistently fails to understand what is being recited in claims 22 and 26 and to respond to all of the subject matter recited by Appellant in claims 22 and 26. In contrast to claims 22 and 26, Lopes does not teach or suggest initially unlocking a piece of office equipment with a password and then timing a "second predetermined period of time" during which the password need not be re-entered if another identifier, as claim, is used" ... This is entirely without reference to any use of a password or a period of time initiated by entry of a password" ... This statement appears to merely refer to the initial use of a password to access a resource without addressing the additionally claimed subject matter of timing a predetermined period of time during which a separate identifier can be used instead of the password to unlock the equipment" ... This difference between the claimed subject matter and the cited prior art is significant, Lopes only teaches the continuous detection of a proximity card authorizing a user to operating a computer. In contrast, Appellant's system does not use or rely on a proximity card, but more flexibly secures a computer or office resource using both a password and an alternative user identifier that can, for a specific time, be used in place of the password".*

The Examiner disagrees with argument, as stated above. 'Lopes teaches using a proximity card to access a system. Lopes also teaches utilizing a timer to monitor the period of time before placing the computer in a locked state. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN The Lopes invention is in addition to the methods already available such as screen savers. It is not a patentable difference that Lopes does not

teach the screen saver functionality, because this is already well know in the art'. In addition Lopes clearly teaches timing a period by which the proximity card is present to enable access.

Regarding Applicant's fifth argument beginning on page 19, directed to claim 23, and 27, "The rejection of claims 23 and 27 should not be sustained for at least the same reasons given above with response to the other independent claims".

The Examiner disagrees with argument, as stated above.

Regarding Applicant's sixth argument beginning on page 20, directed to claim 23, and 27, *"Additionally, at long last, the Examiner has conceded that Lopes does not teach or suggest the claimed "lock control [that] is activated to unlock said equipment upon presentation of an identifier of an authorized user to a sensor of said lock control device" wherein said identifier comprises a credit card." ... Thus, Koll merely teaches the traditional use of a credit card as a means of paying for services which are then allowed in an automated environment. Koll clearly does not teach or suggest the subject matter for which it was cited, i.e., the claimed use of a credit card solely as an "identifier" that identifies a specific user who has previously been designated as an authorized user of the system".*

The Examiner disagrees with argument Koll teaches that the credit card is an identifier see col. 16, lines 16-21 "In an exemplary embodiment, a customer can purchase, and/or re-value/transfer value or otherwise re-value and/or obtain a valid "ready-to-use" form of ID (to activate a system 500). For example, a customer can present credit card, cash, coin, or other currency means and obtain a debit card, smart card or other ID form. Access to products and services from the vending machines controlled by way of network 600 can then be obtained with the valid form of ID". The debit card is considered equivalent to a smart card as an ID form to access a system.

Regarding Applicant's seventh argument beginning on page 21, directed to claim 23, and 27, *"Moreover, the teaching of Lopes and Koll are entirely unrelated. Lopes teaches a secured system in which a proximity card*

identifying an authorized user must be continuously present for access to the system to be granted. (Lopes, abstract). Koll teach and automated "unmanned" business center in which anyone can pay for access to resources with, for example, a credit card, regardless of that person's identity. (Koll, col. 5, lines 33-43). Taken together, these two references clearly do not equate to the subject matter recited by the Appellant in claims 23 and 27."

Examiner disagrees with argument both references are directed to protecting access to a computer based on presentation of an ID. A credit card is another form of ID.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/ELLEN TRAN/
Primary Examiner, Art Unit 2134

Conferees:

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135